IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

In Re: Heartland Payment Systems, Inc. Customer Data Security Breach Litigation	:	4:09-md-02046
	:	MDL No. 2046
	:	Hon. Lee H. Rosenthal
This Document Relates to:	:	CLASS ACTION
The Financial Institution Track Actions	:	JURY TRIAL DEMANDED

MASTER COMPLAINT ON BEHALF OF THE FINANCIAL INSTITUTION PLAINTIFFS

Richard L. Coffman
Texas Bar No. 04497460
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Suite 505
Beaumont, TX 77701
Phone: 409-833-7700
RC@cofflaw.com

Michael A. Caddell
Texas Bar No. 03576700
CADDELL & CHAPMAN
1331 Lamar, # 1070
Houston, TX 77010
Phone: 713-751-0400
Fax: 713-751-0906
MAC@caddellchapman.com

Joseph G. Sauder
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 W. Lancaster Avenue
Haverford, PA 19041
Phone: 610-642-8500
Fax: 610-649-3633
JGS@Chimicles.com

Interim Co-Lead Counsel on Behalf of The Financial Institution Plaintiffs

[Additional Counsel on Signature Page]

The putative Financial Institution Class Representatives[1] (hereinafter, "FI Plaintiffs"), on behalf of themselves and all others similarly situated, by and through the undersigned attorneys, allege as follows:

INTRODUCTION

1. This is a class action lawsuit brought by the FI Plaintiffs, individually, and on behalf of similarly situated banks, credit unions and other financial institutions that were injured as a result of a massive breach in the computer systems (the "Data Breach") at Defendant Heartland Payment Systems, Inc. ("Heartland").

2. Heartland processes credit card and debit card transactions and provides other financial services for over 250,000 businesses across the United States, including restaurants and retail stores. Heartland handles approximately 100 million credit card and debit card transactions per month, totaling over $80 billion worth of transactions per year. Heartland is the fifth largest payment processor in the United States, and the ninth largest in the world.

3. In connection with its payment processing operations, Heartland comes into the possession of – and is entrusted with – the confidential financial information of millions of consumers. Heartland holds itself out to the public as having particular skills and knowledge in the field of

[1] As set forth below, the FI Plaintiffs, who also are the proposed representatives of the National Class and alternative State Sub-Classes, are Amalgamated Bank, Matadors Community Credit Union, Lone Star National Bank, N.A., Elevations Credit Union, First Bankers Trust Company, PBC Credit Union, O Bee Credit Union, Seaboard Federal Credit Union, and the Pennsylvania State Employees Credit Union.

safeguarding such confidential information. Indeed, Heartland would not otherwise be entrusted with such sensitive information in order to process the credit card and debit card transactions of its merchant clients.

4. For example, prior to the Data Breach, Heartland made numerous affirmative misrepresentations concerning the measures that it purportedly had in place to protect the confidential financial information from unauthorized disclosure. Leading up to the Data Breach, Heartland publicly touted its "multiple layers of security to isolate our databases from unauthorized access," represented that it placed "significant emphasis on maintaining a high level of security in order to protect the information of our merchants and their customers," touted its "state-of-the-art" security measures and facilities, and claimed to "limit sharing of non-public personal information to that necessary to complete the transactions on behalf of the consumer and the merchant and [to the extent permitted by law]."

5. Beginning at least as early as December 26, 2007, however, unauthorized persons hacked into Heartland's computer network and gained access to confidential financial data associated with approximately 130 million credit cards and debit cards (*i.e.*, the "Data Breach"). The Heartland Data Breach is reportedly the largest data breach ever to occur in the United States.

6. The sensitive financial information compromised by the Data Breach includes data from credit cards and debit cards that FI Plaintiffs

issued to their customers. As a direct and proximate result of the Data Breach – and after being notified of the Data Breach by Visa and/or MasterCard – FI Plaintiffs re-issued new credit cards and debit cards to their customers. Given the magnitude of the Data Breach, the FI Plaintiffs' expenses to re-issue the cards are substantial and include, *inter alia*, costs for purchasing new plastic credit cards and debit cards, postage and other mailing expenses, time spent by employees addressing this issue, reimbursement of fraudulent charges incurred by customers, and harm to the FI Plaintiffs' reputation and goodwill.

7. To add insult to injury – and contrary to its public assurances concerning the security of the sensitive data with which it was entrusted – immediately after the public disclosure of the Data Breach in January 2009, Robert H.B. Baldwin, Jr., Heartland's President and Chief Financial Officer, was reported saying that "there are a host of things we didn't go into that we're implementing, some larger, some smaller…" and "[c]learly we need to do more [to secure this information]." Following initial investigations into the Data Breach by third parties, Heartland was temporarily removed from Visa's list of payment processors because of, among other things, its non-compliance with the PCI-DSS data security standards. Heartland's acquiring banks also were assessed substantial fines by both Visa and MasterCard. According to Heartland CEO and Chairman of the Board, Robert Carr, the MasterCard fines were levied "ostensibly because of an alleged failure by

Heartland to take appropriate action upon having learned that its computer system may have been breached and upon thereafter having discovered the intrusion."

8. FI Plaintiffs bring this lawsuit for the purpose of recovering, *inter alia*, (i) the out-of-pocket expenses associated with notifying their customers of the Data Breach, (ii) the costs associated with canceling and destroying the credit cards and debit cards containing confidential data that was compromised by the Data Breach, and reissuing new cards to replace those cards that can no longer be used; and (iii) all losses incurred from the unauthorized use of the credit cards and debit cards compromised by the Data Breach.

9. FI Plaintiffs seek relief for Heartland's negligence, breach of contracts to which FI Plaintiffs were intended third-party beneficiaries, breach of implied contracts with FI Plaintiffs, violations of the New Jersey Consumer Fraud Act, violations of various groups of substantially identical state consumer protection and unfair trade practices acts, negligence *per se*, negligent misrepresentation, intentional misrepresentation, and other wrongful acts.

PARTIES

10. Defendant Heartland is a Delaware corporation with its principal place of business located at 90 Nassau Street, Princeton, New Jersey 08542.

11. Plaintiff Amalgamated Bank ("Amalgamated") is a financial institution with its principal place of business in New York, New York. In addition, Amalgamated has a license to do banking business in New Jersey, and has a New Jersey branch. Credit cards and/or debit cards issued by Amalgamated were compromised by the Heartland Data Breach, thereby causing injuries to Amalgamated.

12. Plaintiff Matadors Community Credit Union ("Matadors") is a financial institution with its principal place of business in Chatsworth, California. Credit cards and/or debit cards issued by Matadors were compromised by the Heartland Data Beach, thereby causing injuries to Matadors.

13. Plaintiff Lone Star National Bank, N.A. ("Lone Star") is a financial institution with its principal place of business in Pharr, Texas. Credit cards and/or debit cards issued by Lone Star were compromised by the Heartland Data Breach, thereby causing injuries to Lone Star.

14. Plaintiff Elevations Credit Union ("Elevations") is a financial institution with its principal place of business in Boulder, Colorado. Credit cards and/or debit cards issued by Elevations were compromised by the Heartland Data Breach, thereby causing injuries to Elevations.

15. Plaintiff First Bankers Trust Company, National Association ("First Bankers") is a financial institution with its principal place of business in Quincy, Illinois. Credit cards and/or debit cards issued by First Bankers

were compromised by the Heartland Data Breach, thereby causing injuries to First Bankers.

16. Plaintiff PBC Credit Union ("PBC") is a financial institution with its principal place of business in West Palm Beach, Florida. Credit cards and/or debit cards issued by PBC were compromised by the Heartland Data Breach, thereby causing injuries to PBC.

17. Plaintiff O Bee Credit Union ("O Bee") is a financial institution with its principal place of business in Tumwater, Washington. Credit cards and/or debit cards issued by O Bee were compromised by the Heartland Data Breach, thereby causing injuries to O Bee.

18. Plaintiff Seaboard Federal Credit Union ("Seaboard") is a financial institution with its principal place of business in Bucksport, Maine. Credit cards and/or debit cards issued by Seaboard were compromised by the Heartland Data Breach, thereby causing injuries to Seaboard.

19. Plaintiff Pennsylvania State Employees Credit Union ("PSECU") is a financial institution with its principal place of business in Harrisburg, Pennsylvania. Credit cards and/or debit cards issued by PSECU were compromised by the Heartland Data Breach, thereby causing injuries to PSECU.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this class action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of

2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than the Defendant. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has subject matter jurisdiction over FI Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has jurisdiction over the pre-trial proceedings in this class action pursuant to 28 U.S.C. § 1407 and by Order of the Judicial Panel on Multidistrict Litigation ("JPML"). FI Plaintiffs hereby reserve all of their rights pursuant to *Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach*, 523 U.S. 26 (1998).

22. This Court has personal jurisdiction over Heartland because it owns and operates a business located within the State of Texas.

23. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) and by order of the JPML.

FACTUAL BACKGROUND

A. Heartland's Payment Processing Services.

24. Heartland describes itself as "one of the nation's largest payment processors delivering credit/debit/prepaid card processing, payroll, check management and payments solutions." Since its founding in 1997, Heartland has grown to service 175,000 merchants at 250,000 business locations nationwide, with 2007 net sales of $1.3 billion. Securities issued by

Heartland are publicly traded on the New York Stock Exchange under the symbol "HPY."

25. Heartland provides payment processing services for credit card and debit card transactions for merchants throughout the United States. In addition, Heartland provides certain other merchant services, including check processing, the sale and rental of terminal equipment, payroll and related tax filing services, prepaid card services, and terminal supplies. As such, Heartland is in the business of supplying information for the guidance of its merchant clients and third party entities—such as the FI Plaintiffs and Class members—that are members of the Visa and MasterCard Networks/Associations.

26. According to Heartland's 2008 Form 10-K filed with the Securities and Exchange Commission ("SEC") on March 19, 2009, "substantially all" of Heartland's revenue is derived from processing and settling Visa and MasterCard bank card transactions for its merchant customers. Visa and MasterCard are corporations comprised of associations of financial institutions that operate credit card and debit card payment networks.

27. Upon information and belief, both Visa and MasterCard have issued and maintain operating regulations and/or bylaws, which set forth the minimum security standards that issuers, acquirers, merchants and their agents (such as Heartland) must meet. As Heartland explained in its last

Form 10-K filed before the Data Breach: "In connection with providing services to the merchants and financial institutions that use our services, we are required by regulations and contracts with our merchants to provide assurances regarding the confidentiality and security of non-public consumer information."

28. A typical credit or debit card transaction made on the Visa or MasterCard network is processed through a merchant (where the initial purchase is made), an acquiring bank (which is typically a financial institution that contracts with a merchant to process its credit card and debit card transactions, and is a member of the Visa and/or MasterCard Associations), a processor (which is an entity such as Heartland that contracts with the acquiring bank to process the transactions), and an issuer (which is a financial institution—like the FI Plaintiffs—that issues credit cards and debit cards to consumers and is a member of the Visa and/or MasterCard associations). When a purchase is made using a credit card or debit card on the Visa network,[2] the merchant seeks authorization from the issuer for the transaction. In response, the issuer informs the merchant whether it will approve or decline the transaction. Assuming the transaction is approved, the merchant processes the transaction and electronically forwards the receipt directly to the acquiring bank. The acquiring bank then

[2] Transactions made on the MasterCard network are identical in all relevant respects. Upon information and belief, the only difference is that in the MasterCard network, the merchant initially seeks authorization/verification from its acquiring bank, which then seeks to be reimbursed by the issuer.

pays the merchant, forwards the final transaction data to the issuer, and the issuer reimburses the acquiring bank. The issuer then posts the charge to the consumer's credit card or debit card account.

29. In accordance with their rules, regulations and operating procedures, both Visa and MasterCard monitor their respective networks for potential fraudulent activity. When suspected fraudulent use of credit cards and/or debit cards is identified, MasterCard notifies affected issuers through a Security Alert. Similarly, Visa sends issuers an alert called a "Compromised Account Management Systems Alert," or "CAMS Alert." Upon information and belief, these alerts generally set forth the type of compromised data, the relevant timeframe of the compromise and a list of card numbers that have been exposed.

30. According to Heartland's 2008 Form 10-K filed in March 2009, the payment processing services performed by Heartland include "facilitating the exchange of information and funds between merchants and cardholders' financial institutions, providing end-to-end electronic payment processing services to merchants, including merchant set-up and training, transaction authorization and electronic draft capture, clearing and settlement, merchant accounting, merchant assistance and support and risk management."

31. In connection with its business, Heartland is provided and entrusted with the confidential financial information of millions of customers whose credit cards and/or debit cards are issued by FI Plaintiffs.

32. Heartland enters into contracts with the merchant customers of its acquiring bank(s) to process their point-of-purchase data. Heartland is generally compensated based on a combination of a percentage of the merchants' gross processing fees, plus a flat fee per transaction. For a $100 purchase that is processed through Heartland's system, Heartland will realize approximately $0.52 in net revenue.

33. Upon information and belief, Heartland has entered into written contracts with two banks that are members of the Visa/MasterCard associations: Key Bank, N.A. and Heartland Bank. Through these contracts, Heartland is able to utilize the Visa/MasterCard associations to provide services to and receive benefits from the "cardholder financial institutions" referenced above (*i.e.,* the FI Plaintiffs).

34. FI Plaintiffs are the banks, credit unions and other financial institutions (*i.e.,* the issuers) that issue credit cards and/or debit cards to consumers.

B. The Heartland Data Breach.

35. Beginning at some point at least as early as December 2007, Heartland's processing system was breached by a hacker. Visa reportedly alerted Heartland about "suspicious activity surrounding certain cardholder accounts" in late October 2008. Heartland's IT team subsequently worked with forensic auditors from the major card brands (*i.e.,* Visa, MasterCard,

American Express and Discover) to try to match the suspicious transactions to Heartland's processing activities.

36. Upon information and belief, the Data Breach occurred on Heartland's proprietary "Passport" application, which is used by Heartland to process credit card and debit card transactions and remit payments to merchants.

37. This investigation led to the discovery of "suspicious files" on January 12, 2009. On January 13, 2009, Heartland uncovered "malicious software that apparently had created those files." Robert H.B. Baldwin, Jr., Heartland's President and Chief Financial Officer, reportedly said that the legacy Heartland network on which the Data Breach occurred handles approximately one billion transactions per year.

38. Heartland first publicly disclosed the breach on January 20, 2009 – amidst the flurry of media attention covering the Presidential Inauguration. In a press release issued that day, Baldwin stated: "[w]e understand that this incident may be the result of a widespread global cyber fraud operation, and we are cooperating closely with the United States Secret Service and Department of Justice."

39. The Data Breach involved Heartland's payment system environment. In its SEC filings, Heartland claims that the breach "involved malicious software that appears to have been used to collect in-transit, unencrypted payment card data while it was being processed by Heartland

during the transaction authorization process." A Heartland spokesperson described the "malware" planted by the hackers as containing "extremely sophisticated code." Malware is malicious computer software that can be programmed to, *inter alia*, identify, store and export information (including credit card and debit card information) on hacked computers.

40. In an interview, Robert Carr, Heartland CEO and Chairman of the Board, described the malware as "[s]niffers [that] were put on the network by bad guys." A sniffer is computer hardware and/or software that can intercept, capture and log traffic passing over a network. The sniffer involved in the Data Breach reportedly targeted Heartland's "authorization switch," which sends unencrypted account data from merchants to card networks and then on to the FI Plaintiffs for approval.

41. Baldwin further explained in an interview that the Data Breach had two parts. The first part consisted of key-logging malware, which was able to penetrate Heartland's firewall (the computer network's security barrier software). Key-logging malware can covertly capture anything typed on an infected computer, such as user names and passwords. A sniffer is similar to key-logging malware, but rather than merely capturing keystrokes, a sniffer can capture entire packets of data on a network.

42. According to Baldwin, in the second part of the Data Breach, the key-logging malware "was able to propagate a sniffer onto some of the machines in our network. And those are what was [sic] actually grabbing the

transactions as they floated over our network." Baldwin said that the malicious sniffer program "was watching the transactions as they moved on to our authorization switch, not in the switch itself."

43. At a meeting of a newly-formed organization called the Payments Processors Information Sharing Council ("PPISC"), Heartland distributed samples of the malware code that it believed were used by the hackers as part of the Data Breach.

44. Heartland later acknowledged in its SEC filings that the information compromised in the Data Breach "included card numbers, expiration dates, and certain other information from the magnetic strip on the back of the payment card (including, for a small percentage of transactions, the cardholder's name)."

C. Heartland's Representations and Omissions Regarding its Security Measures.

45. Both before and after the Data Breach, Heartland assured FI Plaintiffs that the sensitive financial information entrusted to Heartland was secure. For example, in the last Form 10-K filed with the SEC before the Data Breach occurred, Heartland made the following affirmative representations concerning its security measures:

- Our internal network configuration provides multiple layers of security to isolate our databases from unauthorized access and implements detailed security rules to limit access to all critical systems.

- In the course of our operations, we compile and maintain a large database of information relating to our merchants and their transactions. We place significant emphasis on maintaining a high

level of security in order to protect the information of our merchants and their customers. We maintain current updates of network and operating system security releases and virus definitions, and have engaged a third party to regularly test our systems for vulnerability to unauthorized access. Further, we encrypt the cardholder numbers that are stored in our databases using triple-DES protocols, which represent the highest commercially available standard for encryption.

- While our operations are subject to certain provisions of these privacy laws, we have limited our use of consumer information solely to providing services to other businesses and financial institutions. We limit sharing of non-public personal information to that necessary to complete the transactions on behalf of the consumer and the merchant and to that permitted by federal and state laws.

46. Prior to the Data Breach, Heartland's website also touted the company's security measures. For example, in describing an "internally-developed, client-server based transaction processing platform" called HPS Exchange, Heartland made the following claims:

Cost, security, and reliability - By operating our own data center, Heartland is able to offer benefits that include:

- Security - Exchange has passed an independent verification process validating compliance with VISA requirements for data security

47. Heartland also claimed on its website that the transactions for which it was responsible "are efficiently processed on all major processing networks including our own, state-of-the-art HPS Exchange." Heartland further claimed that its "success is the result of the combination of a superior long-term customer relationship sales model and the premier technology processing platform in the industry today."

48. In 2006, Heartland created the "Merchant Bill of Rights," which the company describes as "an industry standard for fairness, honesty and transparency in credit and debit card processing." According to its website, "[a]t Heartland, we believe you have the right to" … "encrypted card numbers and secure transactions" and "real-time fraud and transaction monitoring." Heartland's webpage devoted to the Merchant Bill of Rights stresses the importance of retaining a payment processor that has adequate security measures in place:

> No merchant ever wants to have the credit, debit and PIN numbers of its customers stolen by hackers. Hundreds of thousands of attempted hacks are foiled every day by large card transaction processors. It takes layers of state-of-the-art security, technology and techniques to safeguard sensitive credit and debit card account information.
>
> Yet, not all merchant acquirers guarantee encrypted card numbers and secure transactions. Many have not implemented the required technology, and if they have, may not have made the financial investment required to completely protect their systems. This puts every merchant at risk – especially small and mid-sized ones who don't have the internal resources to ensure their customers are protected. It also puts the millions of consumers who use credit and debit cards at risk … with possibly devastating consequences. Robust security is a must – not an option.
>
> Small and mid-sized merchants have the right to encrypted card numbers and secure transactions.[3]

49. Heartland's Bill of Rights is not limited to soliciting business from merchants. Rather, it expressly was designed to assure the public at large that, *inter alia*, Heartland had adequate security measures in place to

[3] http://www.merchantbillofrights.com.

protect the sensitive financial data entrusted to it. Indeed, Heartland made the following remark about its Merchant Bill of Rights in its 2008 Annual Report:

> Through our Merchant Bill of Rights, we are widely recognized as an unrelenting advocate for merchants. Our advocacy extends to the general public, and we will do everything possible to uphold this commitment as we move forward.

50. Even after the Data Breach occurred, Heartland continued to provide FI Plaintiffs and Class members with assurances that it was adequately protecting the sensitive financial information with which it was entrusted. For example, the website that Heartland created in connection with its disclosure of the Data Breach claims that "Heartland is deeply committed to maintaining the security of cardholder data, and we will continue doing everything reasonably possible to achieve this objective."[4]

51. Upon information and belief, the phrases "The Highest Standards" and "The Most Trusted Transactions" have been listed below the Heartland name as part of its corporate logo for several years.

52. In addition to the express, affirmative statements above, by accepting and agreeing to process the credit cards and/or debit cards issued by FI Plaintiffs, Heartland impliedly agreed that it would adequately protect the sensitive information contained in these cards, as well as comply with applicable standards to safeguard data.

[4] http://www.2008breach.com.

D. After the Data Breach was Revealed, Heartland's Sponsoring Banks Were Fined and Temporarily Removed from the List of PCI-DSS Compliant Companies.

53. The Payment Card Industry Data Security Standards (commonly referred to as "PCI-DSS") is a set of requirements for enhancing payment account data security designed to reduce the likelihood of a data breach occurring. According to a statement released by Visa pertaining to the Data Breach, "[c]ompliance with the PCI DSS has significantly reduced unauthorized access to cardholder data." On information and belief, merchants accepting Visa and MasterCard are required to use processors that are PCI compliant, or risk paying fines themselves.

54. The PCI-DSS standards are set by an organization called the Payment Card Industry Security Standards Council (the "PCI Security Standards Council"). The PCI-DSS standards are essentially a checklist of measures for card processors and merchants, and include requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

55. In order to be considered PCI compliant, an applicant must be periodically audited and approved by a third party security vendor. These independent assessment entities, which are typically selected by the entity being audited with selection criteria (usually based on which submits the lowest bid), are known in the industry as Quality Security Assessors, or QSAs. Assuming the QSA is adequately qualified and not been restricted or

impaired in performing its auditing function by the entity being audited, its determination that an entity is PCI compliant is tantamount to a finding that during the snap shot in time when the audit was performed, the company allegedly met the standards.

56. Heartland executives were well aware before the Data Breach occurred that the bare minimum PCI-DSS standards were insufficient to protect it from an attack by sophisticated hackers. For example, on a November 4, 2008 Earnings Call with analysts, Carr remarked that "[w]e also recognize the need to move beyond the lowest common denominator of data security, currently the PCI-DSS standards. We believe it is imperative to move to a higher standard for processing secure transactions, one which we have the ability to implement without waiting for the payments infrastructure to change." Carr's comment confirms that the PCI standards are minimal, and that the actual industry standard for security is much higher.

57. In the aftermath of the Data Breach, Visa conducted its own investigation into Heartland's security measures, after which Visa concluded that Heartland "is in violation of the Visa operating regulations." Consequently, on or around March 14, 2009, Visa removed Heartland from its published list of PCI-DSS compliant service providers. On March 19, 2009, Visa issued a statement indicating that merchants and other card-payment-accepting enterprises may continue to do business with Heartland

without threat of fines from Visa, so long as Heartland continues to work on revalidating its PCI compliance status, or if the merchant's PCI-DSS validation requirements are satisfied.

58. In addition to removing Heartland from its PCI-DSS compliance list, Visa also reportedly put Heartland on probationary status. Under the terms of this probation, Visa reportedly subjected Heartland to more-stringent security assessments, monitoring and reporting, and levied fines on Heartland's sponsoring banks.

59. Visa was not the only entity to sanction Heartland for its conduct related to the Data Breach. On a May 7, 2009 Earnings Call with Analysts, Carr revealed that MasterCard fined Heartland's "sponsor banks[,] ostensibly because of an alleged failure by Heartland to take appropriate action upon having learned that its computer system may have been breached and upon thereafter having discovered the intrusion."

60. For the first quarter 2009, Heartland took a $12.6 million charge related to "expenses and accruals attributable" to the Data Breach, including the fines assessed on Heartland's sponsor banks. MasterCard's fine alone reportedly was in excess of $6 million. In a recent SEC filing, Heartland stated that the Data Breach has cost it $32 million as of June 30, 2009.

61. Heartland claims that it was recertified as PCI compliant by an auditor in April 2009. It remains to be seen, however, whether Heartland

was actually in compliance with the PCI standards when the Data Breach occurred, or if it was more concerned with simply hiring the cheapest QSA so that it could essentially "buy" a "compliance" audit. In a March 19, 2009 speech at the Global Security Summit hosted by Visa in Washington D.C., Visa's Chief Enterprise Risk Officer, Ellen Richey, reportedly said that the Heartland Data Breach would not have occurred had the company had been vigilant about maintaining its PCI compliance, observing that "[n]o compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach."

62. Richey also attributed the Data Breach to Heartland's lack of ongoing vigilance:

> "As we've all read, [Heartland] had validated PCI compliance. But it was the lack of ongoing vigilance in maintaining compliance that left the company vulnerable to attack. Based on our findings following the compromise, Visa has taken the necessary step of removing Heartland from its online list of PCI DSS compliant service providers."

E. Indictments Following the Data Breach.

63. On or around August 17, 2009, the U.S. Department of Justice secured an indictment from a Grand Jury empanelled in Newark, New Jersey against three individuals related to the Data Breach. *United States of America v. Gonzalez, et al.,* No. 1:09-cr-00626-JBS (D.N.J.). One of the

indicted defendants is Albert Gonzalez ("Gonzalez"), a Miami resident; the other two unnamed conspirators reside "in or near Russia."[5]

64. The indictment alleges that between approximately October 2006 and May 2008, the defendants conspired with each other in Mercer County, New Jersey, Morris County, New Jersey and elsewhere to hack into the computer networks of Heartland and other companies in order to steal credit card and debit card numbers. Once obtained, the data was allegedly broken into batches suitable for wholesale distribution over the Internet, and offered for sale.

65. After hacking into the networks, the co-conspirators installed sniffer programs that captured credit card and debit card numbers on a real-time basis as they moved through the networks. The co-conspirators also allegedly placed unique malware, called "Back Doors," on the hacked networks that permitted them to re-access the networks at a later date. The co-conspirators concealed their efforts to hack into computer networks by programming the malware to evade detection by anti-virus software, and erase computer files that would otherwise evidence their unauthorized presence on the networks.

66. According to the indictment, Heartland was the victim of a "SQL Injection Attack" beginning on or around December 26, 2007, which resulted in malware being placed on its payment processing system and the theft of

[5] The indictment also mentions a fourth co-conspirator ("P.T."), who the federal government has not named as a defendant.

more than 130 million credit card and debit card numbers and "corresponding Card Data." A SQL ("Structured Query Language") Injection Attack is a method of hacking into and gaining unauthorized access to computers connected to the Internet.

67. On or around August 25, 2009, Gonzalez pled guilty to charges filed against him in a similar indictment for another data breach in the United States District Court for the District of Massachusetts. *United States v. Albert Gonzalez,* No. 08-CR-10223-PBS (D. Mass.). The plea agreement states that "over 40,000,000 credit and debit card numbers stolen during the offenses were recovered."

F. Heartland's Conduct After the Data Breach.

68. Upon information and belief, on the day after the Data Breach, Heartland conducted a webinar (a conference call held via the internet) about the Data Breach for its high level employees, sales representatives and/or relationship managers. Upon information and belief, Heartland relationship managers were told that PCI compliance was not a big deal.

69. One of Heartland's relationship managers resigned on or around April 23, 2009, in part because of Heartland's statements regarding its PCI compliance. A Referee's Decision in a Delaware Department of Labor proceeding reached the conclusion that this relationship manager had "good cause" to leave her position at Heartland based, in part, on Heartland's conduct.

70. For what has been described as potentially the "largest data breach ever" – and which undisputedly includes sensitive financial and banking information – Heartland has publicly taken a cavalier approach regarding the Data Breach. Indeed, in a January 2009 article in *The Washington Post*, Baldwin described the breach as follows:

> "The nature of the [breach] is such that card-not-present transactions are actually quite difficult for the bad guys to do because one piece of information we know they did not get was an address," Baldwin said. As a result, he said, the prospect of thieves using the stolen data to rack up massive amounts of fraud at online merchants "is not impossible, but much less likely."

71. Many states have laws that require entities like Heartland to promptly notify affected consumers when their sensitive financial data is compromised in a data breach. Upon information and belief, Heartland has not provided *any* individualized notice (other than in its press releases and websites) to *any* consumers who were affected by the Data Breach. Instead, Heartland has effectively shifted this obligation (and substantial expense and time associated therewith) to FI Plaintiffs, which have re-issued compromised credit cards and/or debit cards to consumers, as well as absorbing millions of dollars of unauthorized charges, expenses and losses.

72. Instead of actively addressing the injuries to FI Plaintiffs that were caused as a result of its negligence and other misconduct, Heartland has turned a blind eye to the situation. Indeed, the Question & Answer section

on Heartland's website instructs consumers to notify *the card issuer* of any suspected unauthorized transactions.

73. It is clear that there are several steps that Heartland should have and could have taken that might have prevented the Data Breach. Significantly, Baldwin reportedly acknowledged as much in an interview conducted immediately after the Data Breach:

> "There are a host of things we didn't go into that we're implementing, some larger, some smaller, all of which are designed to say, 'OK, we had a commitment to high security. We were PCI compliant -- that was certified in April of last year. Yet we had this problem. Clearly we need to do more.' So our IT team is implementing as many additional precautions as it can as quickly as possible."

74. On its website related to the Data Breach, Heartland states – now that its processing systems were breached – that it is taking numerous precautions going forward:

> **What are we doing to further secure our systems?** Heartland immediately took a number of steps to further secure its systems. In addition, Heartland will implement a next-generation program designed to flag network anomalies in real-time and enable law enforcement to expeditiously apprehend cyber criminals. Heartland is deeply committed to maintaining the security of cardholder data, and we will continue doing everything reasonably possible to achieve this objective.

75. Heartland is currently in the process of implementing an end-to-end encryption process called "E3." This initiative is designed to encrypt credit card and debit card data from the moment the card is swiped by the merchant until it arrives at its final destination at the issuer for

authorization and settlement. In a January 27, 2009 press release, Heartland stated that it had created an "internal department dedicated exclusively to the development of end-to-end encryption to protect merchant and customer data used in financial transactions." On an August 4, 2009 Earnings Call with analysts, Carr stated that the E3 end-to-end encryption project will "offer merchants the highest level of beta security in the marketplace." And, according to a June 17, 2009 press release issued by Heartland, the E3 software "will significantly enhance the security of payment card information throughout the processing lifecycle."

76. On information and belief, before the E3 project, Heartland did not engage in end-to-end encryption because of the expense to do so and its potential negative impact on Heartland's earnings.

77. Carr also stated on the August 4th call that Heartland had incurred $19.4 million in costs related to the Data Breach for the second quarter 2009, the majority of which relate to "a settlement offer we made in an attempt to resolve certain of the processing system intrusion claims." Carr, however, refused to disclose to whom Heartland had extended the settlement offer.

G. The Injuries to the FI Plaintiffs and Class Members.

78. FI Plaintiffs are financial institutions that, after being notified of the Data Breach, were forced to cancel, destroy and re-issue credit cards and/or debit cards to their customers. As a direct and proximate result of the

Data Breach and Heartland's improper conduct pertaining to the Data Breach, FI Plaintiffs and the Class members suffered actual financial injuries in the form of, *inter alia*, the costs to cancel, destroy and re-issue to their customers credit cards and/or debit cards compromised by the Data Breach, and the reimbursement of fraudulent charges made on compromised cards.

79. As with the FI Plaintiffs named herein as the putative Class Representatives, the unnamed, similarly situated financial institutions (*i.e.*, the Class members) have suffered (and continue to suffer) similar and substantial out-of-pocket damages due to Heartland's above negligent and wrongful conduct.

CLASS ACTION ALLEGATIONS

80. The FI Plaintiffs bring this action as a class action, pursuant to FED. R. CIV. P. 23(a), 23(b)(1), 23(b)(2) and/or 23(b)(3), on behalf of themselves and the following nationwide class:

> All banks, credit unions, financial institutions and other entities in the United States that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**Nationwide Class**").

81. Pursuant to FED. R. CIV. P. 23(c)(5), and in the alternative to certifying the Nationwide Class, FI Plaintiffs, in Counts VIII through X below, seek to certify and represent a sub-class of similarly situated credit card and/or debit card issuing banks, credit unions and other financial

institutions in states that have consumer protection and/or unfair trade practice statutes substantially identical in all relevant respects (the "**State Statutory Sub-Classes"**).

82. Pursuant to FED. R. CIV. P. 23(c)(5), and in the alternative to certifying the Nationwide Class and/or the State Statutory Sub-Classes with substantially identical consumer protection and/or unfair trade practice statutes, FI Plaintiffs seek to certify and represent the following nine (9) specific **State Sub-Classes**:

> All banks, credit unions, financial institutions and other entities in California that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**California Sub-Class**").

> All banks, credit unions, financial institutions and other entities in Texas that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**Texas Sub-Class**").

> All banks, credit unions, financial institutions and other entities in Colorado that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**Colorado Sub-Class**").

All banks, credit unions, financial institutions and other entities in Illinois that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**Illinois Sub-Class**").

All banks, credit unions, financial institutions and other entities in Florida that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**Florida Sub-Class**").

All banks, credit unions, financial institutions and other entities in Washington that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**Washington Sub-Class**").

All banks, credit unions, financial institutions and other entities in New York that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**New York Sub-Class**").

All banks, credit unions, financial institutions and other entities in Maine that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**Maine Sub-Class**").

> All banks, credit unions, financial institutions and other entities in New Jersey that issued credit cards and/or debit cards; received a Visa and/or MasterCard alert or were otherwise notified that such credit cards and/or debit cards were compromised by the Heartland Data Breach; and re-issued compromised credit cards and/or debit cards, and/or absorbed unauthorized charges on compromised cards. (the "**New Jersey Sub-Class**").

Collectively, the California, Texas, Colorado, Illinois, Florida, Washington, New York, Maine and New Jersey Sub-Classes shall be referred to as the "**State Sub-Classes**."

83. Excluded from the proposed National Class and/or each Sub-Class are Heartland and its parent corporations, subsidiary corporations, affiliates, agents and representatives.

84. Upon information and belief, the proposed National Class and/or each Sub-Class consists of thousands of geographically dispersed members, the joinder of which in one action is impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

85. The rights of each member of the proposed National Class and/or each Sub-Class were violated in a similar fashion based upon Heartland's uniform wrongful actions and/or inaction.

86. The following questions of law and fact are common to each proposed Class and/or Sub-Class and predominate over questions that may affect individual Class members:

A. whether Heartland was negligent in collecting, storing and otherwise profiting from its access to the sensitive financial data of the customers of the FI Plaintiffs and Class members;

B. whether Heartland owed one or more duties to FI Plaintiffs and the Class members to protect the sensitive financial data of their customers;

C. whether Heartland breached its duty to exercise reasonable care in protecting the sensitive financial data of the customers of the FI Plaintiffs and the Class members;

D. whether Heartland's conduct violates the consumer protection and/or unfair trade practice statutes of the states in the State Statutory Sub-Class;

E. whether Heartland's conduct proximately caused damages to FI Plaintiffs and the Class members;

F. whether FI Plaintiffs and the Class members are entitled to compensation, monetary damages and/or any other services/corrective measure(s) from Heartland and, if so, the nature and amount of any such relief; and

G. whether statutory, punitive and/or treble damages are proper in this matter.

87. The FI Plaintiffs will fairly and adequately represent and protect the interests of the proposed Nationwide Class and/or each Sub-Class

they are designated to represent. The FI Plaintiffs have no interests that are antagonistic to and/or that conflict with the interests of other putative Class members.

88. The FI Plaintiffs have retained counsel competent and experienced in the prosecution of data breach litigation, complex commercial litigation and class action litigation.

89. Heartland has acted or refused to act on grounds generally applicable to the proposed Nationwide Class and/or each Sub-Class, thereby making appropriate equitable relief with respect to the Nationwide Class and/or each Sub-Class.

90. A class action is superior to all other available methods for the fair and efficient adjudication of the claims of the FI Plaintiffs and the Class members. FI Plaintiffs and the Class members have suffered (and continue to suffer) irreparable harm (including damages to reputation and goodwill) as a result of Heartland's negligent and unlawful conduct. The damages suffered by some of the FI Plaintiffs and Class members may be relatively small. As such, many individual Class members cannot afford to seek legal redress on an individual basis for the wrongs complained of herein. Absent a class action, many Class members who suffered damages as a result of the Data Breach will not be adequately compensated.

91. Members of the proposed Nationwide Class and each Sub-Class are readily ascertainable. By definition, they have all been notified that

certain credit cards and/or debit cards issued by them were compromised by the Heartland Data Breach, and replaced credit cards and/or debit cards on that list of compromised cards.

92. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Heartland. Moreover, adjudications with respect to individual Class members would, as a practical matter, be dispositive of the interests of the other Class members.

93. In the alternative to full certification, FI Plaintiffs seek certification of the following issues pursuant to FED. R. CIV. P. 23(c)(4): (i) was Heartland negligent and/or did it otherwise engage in misconduct in connection with the Data Breach, (ii) did Heartland's negligence and/or misconduct directly and/or proximately result in the Data Breach, and (iii) did the Data Breach directly and/or proximately cause injuries to FI Plaintiffs and the Class members?

CLAIMS AND CAUSES OF ACTION

COUNT I

Breach of Contracts to Which FI Plaintiffs and the Class Members were Intended Third-Party Beneficiaries (on behalf of the Nationwide Class under New Jersey law or, alternatively, on behalf of each of the State Sub-Classes)

94. The preceding factual statements and allegations are incorporated herein by reference.

95. Upon information and belief, FI Plaintiffs and the Class members are intended third-party beneficiaries of contracts entered into between Heartland and various entities including, without limitation, (i) contracts between Heartland and its merchant customers to process credit card and/or debit card transactions, (ii) contracts between Heartland and Visa and/or MasterCard (including their operating regulations), and (iii) contracts between Heartland and Key Bank and Heartland Bank, its acquiring banks.

96. Upon further information and belief, these contracts and regulations require, *inter alia*, that Heartland take appropriate steps to safeguard the sensitive financial information of the customers of the FI Plaintiffs and Class members.

97. FI Plaintiffs and the Class members are intended third party beneficiaries of these contracts and regulations. Under the circumstances, recognition of a right to performance by FI Plaintiffs and the Class members is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give FI Plaintiffs and the Class members the benefit of the performance promised in the contracts.

98. Heartland breached these agreements by, *inter alia*, failing to adequately safeguard this sensitive financial information of the customers of

FI Plaintiffs and the Class members, which directly and/or proximately caused FI Plaintiffs and the Class members to suffer substantial damages.

99. Upon further information and belief, Heartland saved (or avoided spending) a substantial sum of money by knowingly failing to comply with its contractual obligations, and continues to do so.

COUNT II

Negligence
(on behalf of the Nationwide Class under New Jersey law or, alternatively, on behalf of each of the State Sub-Classes)

100. The preceding factual statements and allegations are incorporated herein by reference.

101. Upon coming into possession of the private, non-public, sensitive financial information of FI Plaintiffs' and the Class members' customers, Heartland had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen. Heartland's duty arises from the common law, in part because it was reasonably foreseeable to Heartland that a breach of security was likely to occur under the circumstances and it would cause damages to the FI Plaintiffs as alleged herein, as well as from the duties expressly imposed upon Heartland from other sources, such as implied contracts between Heartland and the Class members, contracts between Heartland and other third parties (such as its acquiring banks), membership in the Visa and MasterCard Networks and industry standards (such as PCI-DSS).

102. Heartland also had a duty to timely disclose to FI Plaintiffs' and the Class members' customers that the Data Breach had occurred and the private, non-public, sensitive financial information of FI Plaintiffs' and the Class members' customers, pertaining to their compromised credit cards and/or debit cards had been, or was reasonably believed to be, compromised. Instead, Heartland shifted its notification obligation to FI Plaintiffs and the Class members. Heartland's duty to disclose the Data Breach to FI Plaintiffs' and the Class members' customers also arise from the above same sources.

103. Heartland also had a duty to put into place internal policies and procedures designed to detect and prevent the unauthorized dissemination of FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their compromised credit cards and/or debit cards. Such duty also arises from the above same sources.

104. Heartland, by and through its above negligent acts and/or omissions, unlawfully breached its duties to FI Plaintiffs and the Class members by, *inter alia*, failing to exercise reasonable care in protecting and safeguarding FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their compromised credit cards and/or debit cards within its possession, custody and control.

105. Heartland, by and through its above negligent acts and/or omissions, further breached its duties to FI Plaintiffs and the Class members by failing to put into place internal policies and procedures designed to detect

and prevent the unauthorized dissemination of FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their compromised credit cards and/or debit cards within its possession, custody and control.

106. But for Heartland's negligent and wrongful breach of the duties it owed (and continues to owe) to FI Plaintiffs and the Class members, the FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their compromised credit cards and/or debit cards would never have been wrongfully disseminated, the Data Breach would not have occurred and FI Plaintiffs and the Class members would not have incurred monetary damages notifying their customers about the Data Breach, canceling, destroying and replacing credit cards and/or debit cards compromised by the Data Breach and/or absorbing unauthorized charges made on their customers' credit cards and/or debit cards.

107. The Data Breach and the above-described substantial injuries suffered by FI Plaintiffs and the Class members as a direct and/or proximate result of the Data Breach were reasonably foreseeable consequences of Heartland's negligence and/or gross negligence.

108. The economic loss doctrine does not apply because, *inter alia*, Heartland is in the business of supplying information for the guidance of others in its business transactions, Heartland made negligent and intentional

misrepresentations, and the FI Plaintiffs and Class members are not in direct privity of contract with Heartland.

COUNT III

Breach of Implied Contract
(on behalf of the Nationwide Class under New Jersey law or, alternatively, on behalf of each of the State Sub-Classes)

109. The preceding factual statements and allegations are incorporated herein by reference.

110. The FI Plaintiffs' and Class members' customers were required to provide Heartland and its agents with their private, non-public, sensitive financial information in order for Heartland to facilitate their credit card and/or debit card transactions. Implicit in this requirement was a covenant requiring Heartland to, *inter alia*, take reasonable efforts to safeguard this information and promptly notify FI Plaintiffs' and Class members' customers in the event their information was compromised. Indeed, Heartland recognizes these obligations because it states on its website that the company is "deeply committed to maintaining the security of cardholder data, and we will continue doing everything reasonably possible to achieve this objective." This covenant also ran (and continues to run) to FI Plaintiffs and the Class members.

111. Similarly, through its public statements regarding its internal security measures, Heartland impliedly promised FI Plaintiffs and the Class members that it would take adequate measures to protect the FI Plaintiffs'

and Class members' customers' private, non-public, sensitive financial information pertaining to their credit cards and/or debit cards from unauthorized dissemination.

112. These implied contracts also required Heartland to not disclose the FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their credit cards and/or debit cards.

113. Notwithstanding its obligations, Heartland knowingly failed to safeguard and protect FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their compromised credit cards and/or debit cards. To the contrary, Heartland allowed this information to be disseminated to unauthorized third parties. Heartland's above wrongful actions and/or inaction breached its implied contracts with FI Plaintiffs and the Class members which, in turn, directly and/or proximately caused FI Plaintiffs to suffer substantial financial injuries.

COUNT IV

Negligence *Per Se*
(on behalf of the Nationwide Class under New Jersey law or, alternatively, on behalf of each of the State Sub-Classes)

114. The preceding factual statements and allegations are incorporated herein by reference.

115. At all relevant times, Heartland was required (and continues to be required) to comply with, *inter alia*, the applicable industry standards

requiring Heartland to implement internal systems controls to prevent, detect and respond to system intrusions, and to securely handle and transfer sensitive financial data. These standards include, without limitation, the PCI-DSS, Visa Operating Regulations and MasterCard Rules.

116. These regulations and industry security standards establish the minimal duty of care owed by Heartland to the FI Plaintiffs and Class members.

117. Heartland knowingly failed to comply with the PCI-DSS as evidenced by Visa's temporary removal of Heartland from its list of PCI compliant processors. Upon information and belief, had Heartland actually been in PCI compliance during the relevant time period, the Data Breach would not have occurred.

118. Heartland's wrongful conduct also violated the Visa Operating Regulations and MasterCard Rules as evidenced by the fines and other sanctions imposed by Visa and MasterCard.

119. Heartland's violations of the Visa and MasterCard regulations and industry security standards constitute negligence *per se* and directly and/or proximately caused FI Plaintiffs and the Class members to suffer substantial injuries.

120. FI Plaintiffs and the Class members were members of the class of persons intended to be protected by these regulations and industry security standards. The injuries suffered by FI Plaintiffs and the Class members

were of the type intended to be prevented by these regulations and industry security standards.

COUNT V

Negligent Misrepresentation
(on behalf of the Nationwide Class under New Jersey Law or, alternatively, on behalf of each of the State Sub-Classes)

121. The preceding factual statements and allegations are incorporated herein by reference.

122. Heartland negligently failed to disclose to FI Plaintiffs and the Class members material facts regarding its computer security systems and the measures it employed to protect FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their compromised credit cards and/or debit cards. Heartland's material omissions were made in the course of Heartland's business for the guidance of others in their business transactions. Heartland also negligently made incorrect statements concerning its security measures, and made false communications of material facts.

123. Heartland knew that by virtue of their membership in the Visa and MasterCard Networks, FI Plaintiffs and the Class members (*i.e.,* issuing banks) relied on Heartland to employ appropriate data security measures.

124. Heartland failed to exercise reasonable care or competence in withholding this information vis-à-vis FI Plaintiffs and the Class members.

125. FI Plaintiffs justifiably relied on Heartland's silence and incorrect statements. That reliance and Heartland's above negligent omissions and statements directly and/or proximately caused FI Plaintiffs and the Class members to suffer serious injuries.

COUNT VI

Intentional Misrepresentation
(on behalf of the Nationwide Class under New Jersey Law or, alternatively, on behalf of each of the State Sub-Classes)

126. The preceding factual statements and allegations are incorporated herein by reference.

127. As set forth above, and in the alternative to the negligent misrepresentation claim, Heartland intentionally withheld the above material information regarding the lack of internal system controls in place to protect FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their compromised credit cards and/or debit cards. Heartland intentionally withheld this information - notwithstanding its duty to speak - with the intent that the FI Plaintiffs and Class members rely on such omissions. Heartland also made material misrepresentations concerning its security measures.

128. Heartland's misstatements and material omissions related to presently existing and/or past facts, were made by Heartland with knowledge of their falsity, and were made by Heartland with the intention that FI Plaintiffs and Class members would reasonably rely on those statements.

129. The FI Plaintiffs and Class members reasonably relied on Heartland's omissions and false statements to their financial detriment (as set forth above).

COUNT VII

Violations of the New Jersey Consumer Fraud Act ("NJCFA") (N.J.S.A. § 56:8-1 *et seq.*) (on behalf of the Nationwide Class under New Jersey law or, alternatively, on behalf of the New Jersey Sub-Class)

130. The preceding factual statements and allegations are incorporated herein by reference.

131. The NJCFA provides a private right of action on behalf of "[a]ny person who suffers any ascertainable loss of moneys or property, real or personal, as a result of the use or employment by another person of any method, act, or practice declared unlawful under this act…" N.J. Stat. § 56:8-19.

132. For purposes of the NJCFA, a "person" is defined to include "any natural person, . . . company, trust, business entity or association . . . ,." N.J. Stat. § 56:8-1(d).

133. FI Plaintiffs and the Class members are "persons" within the meaning of the NJCFA. FI Plaintiffs and the Class members are consumers in the marketplace for, *inter alia*, credit card and/or debit card transaction processing services, and have been injured in this capacity. In the alternative, FI Plaintiffs and the Class members are commercial competitors of Heartland.

134. At all relevant times material hereto, Heartland conducted trade and commerce in New Jersey and elsewhere within the meaning of the NJCFA.

135. Heartland has engaged (and continues to engage) in deceptive acts and practices in violation of the NJCFA by *inter alia,* making materially false and misleading statements and/or omissions and engaging in unconscionable commercial practices regarding the measures it allegedly employed to safeguard FI Plaintiffs' and Class members' customers' private, non-public, sensitive financial information pertaining to their credit cards and/or debit cards.

136. FI Plaintiffs and the Class members suffered (and continue to suffer) an ascertainable loss of monies as a direct and/or proximate result of Heartland's past and ongoing violations of the NJCFA.

COUNT VIII

Violations of State Statutes Broadly Prohibiting Unfair Acts or Practices (on behalf of FI Plaintiffs and State Statutory Sub-Class and/or State Sub-Class members in California, Connecticut, Florida, Hawaii, Illinois, Massachusetts, Missouri, Nebraska, Oklahoma, Rhode Island, Vermont, and/or Washington)

137. The preceding factual statements and allegations are incorporated herein by reference.

138. The following state statutes broadly prohibit unfair or deceptive acts or practices:

- Cal. Bus. & Prof. Code § 17200, et seq.

- Conn. Gen. Stat. § 42-110b(a)
- Fla. Stat. § 501.204(1)
- Haw. Rev. Stat. § 480-2(a)
- 815 Ill. Comp. Stat. § 505/2
- Mass. Gen. Laws ch. 93A, § 1, et seq.
- Mo. Rev. Stat. § 407.020(1)
- Neb. Rev. Stat. § 59-1602
- Okla. Stat. tit. 15, § 753(20)
- R.I. Gen. Laws § 6-13.1-2 ; R.I. Gen. Laws § 6-13.1-1(6)
- Vt. Stat. Ann. tit. 9, § 2453(a)
- Wash. Rev. Code § 19.86.020

139. By virtue of its above wrongful acts and/or omissions, Heartland has engaged (and continues to engage) in unfair acts and practices in violation of the foregoing statutes, all of which are substantially identical in all relevant respects. Heartland's wrongful acts and/or omissions in violation of these statutes directly and/or proximately caused FI Plaintiffs and the Class members to suffer the substantial injuries set forth above.

COUNT IX

Violations of State Statutes Broadly Prohibiting
False, Misleading, or Deceptive Acts or Practices
(on behalf of FI Plaintiffs and State Statutory Sub-Class and/or State Sub-Class members in Arkansas, Colorado, Delaware, Washington, D.C., Idaho, Minnesota, Nevada, New Jersey, New Mexico, New York and/or North Dakota)

140. The preceding factual statements and allegations are incorporated herein by reference.

141. The following state statutes broadly prohibit false, misleading and/or deceptive acts or practices:

- Ark. Code § 4-88-107(a)(10); Ark. Code § 4-88-108(1)
- Colo. Rev. Stat. § 6-1-105(1)(l)
- Del. Code, tit. 6, § 2513(a)
- D.C. Code § 28-3904(e)
- Idaho Code § 48-603(17)
- Minn. Stat. § 325F.69 subdiv. 1
- Nev. Rev. Stat. § 598.0915
- N.J. Stat. Ann. § 56:8-2
- N.M. Stat. Ann. § 57-12-3; N.M. Stat. Ann. § 57-12-2(D)
- N.Y. Gen. Bus. Law § 349(a)
- N.D. Cent. Code § 51-15-02

142. By virtue of its above wrongful acts and/or omissions, Heartland has engaged (and continues to engage) in unfair, deceptive, false and misleading conduct in violation of the foregoing statutes, all of which are

substantially identical in all relevant respects. Heartland's wrongful acts and/or omissions in violation of these statutes directly and/or proximately caused FI Plaintiffs and the Class members to suffer the substantial injuries set forth above.

COUNT X

Violations of State Statutes Broadly Prohibiting Unconscionable Acts or Practices (on behalf of FI Plaintiffs and State Statutory Sub-Class and/or State Sub-Class members in Arkansas, Florida, Idaho, New Jersey, New Mexico and/or Texas)

143. The preceding factual statements and allegations are incorporated herein by reference.

144. The following state statutes broadly prohibit unconscionable acts or practices:

- Ark. Code § 4-88-107(a)(10)
- Fla. Stat. § 501.204
- Idaho Code § 48-603(18)
- N.J. Stat. Ann. § 56:8-2
- N.M. Stat. Ann. § 57-12-3; N.M. Stat. Ann. § 57-12-2(E);
- Tex. Bus. & Com. Code § 17.50(a)(3); Tex. Bus. & Com. Code § 17.45(5) (on behalf of FI Plaintiffs with assets of less than $25 million).

145. By virtue of its above wrongful acts and/or omissions, Heartland has engaged (and continues to engage) in unconscionable acts or practices in violation of the foregoing statutes, all of which are substantially identical in

all relevant respects. Heartland's wrongful acts and/or omissions in violation of these statutes directly and/or proximately caused FI Plaintiffs and the Class members to suffer the substantial injuries set forth above.

PRAYER FOR RELIEF

WHEREFORE, the FI Plaintiffs, individually and on behalf of the National Class members and/or members of the alternative Sub-Classes, respectfully request that (a) Heartland be required to appear and answer this lawsuit, (b) this action be certified as a class action, (c) FI Plaintiffs be designated the Class Representatives, and (d) FI Plaintiffs' Interim Co-Lead Counsel be appointed as Class Counsel. FI Plaintiffs, individually and on behalf of the National Class members and/or members of the alternative Sub-Classes, further request that upon final trial or hearing, judgment be awarded against Heartland for:

(i) actual damages to be determined by the trier of fact;

(ii) pre- and post-judgment interest at the highest legal rates applicable;

(iii) appropriate injunctive and/or declaratory relief;

(iv) reasonable attorneys' fees and litigation expenses incurred through the trial and any appeals of this case;

(v) punitive damages, treble damages, and statutory damages;

(vi) costs of suit; and

(vii) such other and further relief that this Court deems just and proper.

JURY DEMAND

FI Plaintiffs respectfully demand a trial by jury on all issues so triable.

Dated: September 23, 2009

Respectfully submitted,

By: /s/ Michael A. Caddell

Michael A. Caddell
Cory S. Fein
CADDELL & CHAPMAN
1331 Lamar, #1070
Houston TX 77010
713.751.0400 (phone)
713.751.0906 (fax)
mac@caddellchapman.com

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Ste. 505
Beaumont, TX 77701
(409) 833-7700
(866) 835-8250
rc@cofflaw.com

Joseph G. Sauder
Matthew D. Schelkopf
Benjamin F. Johns
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 West Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633
JGS@chimicles.com

Interim Co-Lead Counsel for the Financial Institution Plaintiffs

Natalie Finkelman
SHEPHERD FINKELMAN
MILLER & SHAH, LLP
35 E State Street
Media, PA 19063

R Douglas Gentile
DOUTHIT FRETS ROUSE
GENTILE & RHODES LLC
903 East 104th St
Ste 610
Kansas City , MO 64131

Christopher G Hayes
LAW OFFICE OF CHRISTOPHER G.
HAYES
225 South Church St
West Chester, PA 19382

Jeffrey L Kodroff
SPECTOR ROSEMAN KODROFF &
WILLIS, P.C.
1818 Market St
Ste 2500
Philadelphia , PA 19103

Mitchell A Toups
WELLER, GREEN, TOUPS &
TERRELL, LLP
PO Box 350
Beaumont, TX 77704

Gregory Weiss
LEOPOLD~KUVIN, P.A.
2925 PGA Blvd
Palm Beach Gardens , FL 33410

John R. Wylie
FUTTERMAN HOWARD WATKINS WYLIE
& ASHLEY, CHTD.
122 S. MICHIGAN AVE., SUITE 1850
CHICAGO, IL 60603

Steering Committee Counsel for the Financial Institution Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that, on September 23, 2009, the foregoing **FIRST MASTER COMPLAINT ON BEHALF OF THE FINANCIAL INSTITUTION PLAINTIFFS** was filed electronically via the Court's ECF system, and thereby served on all counsel of record.

/s/ Cory S. Fein
Cory S. Fein